

DESCRIPTION

**A TIME-OF-FLIGHT MEASUREMENT SYSTEM AND A METHOD OF
OPERATING THE SYSTEM**

5

The present invention relates to improvements in or relating to systems which make time-of flight measurements and to applications using such systems. A particular, but not exclusive application of the present invention is in keyless entry systems, for example passive keyless entry systems used in
10 the automotive market.

For convenience of description, the present invention will be described with reference to vehicle entry systems.

Philips Semiconductors in a document number 9397 750 10317,
15 released October 2002, and available on
<http://www.semiconductors.philips.com/acrobat/literature/9397/75010317.pdf>,
discloses a vehicular passive keyless entry system. A block schematic
diagram of this known passive keyless entry system is shown in Figure 1 of the
accompanying drawings. The system comprises a vehicle mounted first part
20 10 and a portable second part 12 which may be incorporated into a key fob,
access card or other suitably small device. The vehicle mounted part 10
comprises a 125 kHz inductive transmitter 14 having a signal output coupled to
an antenna 16 in the form of an inductive coil. The transmitter 14 is operative
at least while the vehicle doors are locked. A microcontroller 18 is provided
25 having an input coupled to an output of the inductive transmitter 14, an
input/output 20 coupled to output locking/unlocking devices (not shown), such
as door locks, boot (or trunk) locks, bonnet (or hood) locks and engine ignition
security devices, and an output coupled to a UHF receiver 22. An antenna 24
is coupled to the receiver.

30

The portable part 12, which constitutes an identification (ID) device,
comprises a 125 kHz LF front end stage 26 having a three dimensional input
consisting of three orthogonally related inductive coils 28. A microcontroller 30

has an input coupled to an output of the front end stage 26 and an output coupled to a UHF transmitter 32 having an antenna 34. The portable part 12 also includes connections for connecting to a battery 36, and on/off switch 38, a wake-up pattern detector 40 and a power management stage 42.

5 The illustrated system allows drivers to enter their vehicles without any explicit action to unlock them as authorization is granted simply by carrying the appropriate portable part or ID device 12. As a driver comes within an operating area, say less than 2.5 m, of the vehicle and places his/her hand on the door handle causing the inductive transmitter 14 to generate a challenge
10 signal. The front end stage 26 receives the challenge signal which causes the portable part 12 to be woken-up. Once woken the microcontroller 30 analyses the challenge signal and once satisfied that it is directed to it, a response signal is compiled, encrypted if thought necessary, and passed to the UHF transmitter 32 for onward transmission to the UHF receiver 22.

15 The microcontroller 18 in the vehicle mounted part 10 compares the signal received by the UHF receiver 22 with internally stored information and, if authentication is successful, unlocks the vehicle door. The entire process takes only a few milliseconds from start to finish

20 As a refinement, once the driver has gained access to the inside of the vehicle, the authentication procedure may be repeated and if successful the engine can be started by simply pressing the start button.

Finally after leaving the vehicle, it can be locked by simply pressing the door handle. Before locking a check is made to ensure that the portable part 12 is outside the vehicle.

25 Since the introduction of such a system a flaw, termed "relay attack" has been discovered whereby two persons equipped with suitable radios capable of transmitting over distances greater than that achievable by the transmitter 32 in the portable part 12 can cheat the system into believing that the vehicle owner is gaining entry to his own vehicle. Figure 2 illustrates diagrammatically
30 how such a relay attack can be effected. A first thief TF1 equipped with two radio transceivers 50, 56 positions himself/herself close to a vehicle 44 containing the vehicle part 10 and a second thief TF2 equipped with two radio

transceivers 52, 54 positions himself/herself close to the vehicle's owner 46 who has the portable part 12 on their person. The first thief TF1 presses the door handle of the vehicle 44 causing the inductive transmitter 14 to generate a challenge signal having a frequency f . Signal frequency f is received by the transceiver 50 and is relayed as frequency f_1 to the transceiver 52 carried by the second thief TF2. The signal is reconverted to the frequency f which is detected by the front end stage 26 in the portable part. The UHF transmitter 32 transmits a UHF signal having a frequency f' which is picked-up by the transceiver 54 and is forwarded as frequency f_2 to the transceiver 56, the latter transceiver converts the signal back to the UHF frequency f' which is transmitted the receiver 22 in the vehicle part 10 causing the microcontroller 18 to unlock the door. If necessary the operation is repeated to enable the vehicle's engine to be started. The owner of the vehicle 44 is unaware of what has happened until he/she returns to find their vehicle missing.

One method which has been proposed to defeat relay attack is to make the system sensitive to an excessive time delay between the generation of, and reception of, signals between the vehicle part 10 and the portable part 12 and inhibit operation of the locks and any other security devices. The excessive time delay occurs due to the extended round trip time by way of the transceivers 50, 52, 54, and 56. Ignoring the additional time of flight due to signal propagation through these transceivers, time-of-flight measurements are subject not only to propagation over the variable distance between the vehicle mounted part and the portable part but also to internal delays incurred by signals through the circuits in the respective vehicle and portable parts. In the case of narrowband systems these internal delays occur between (1) the antenna and the IF or baseband parts of the transmitter and (2) the antenna and the IF or baseband parts of the receiver. There are two categories of these internal delays, namely, analogue delays and digital delays. The analogue delays are expressed by the group delays of the individual elements in the signal chain. Ideally group delays should be constant across the bandwidth of the signal. However this is not the case because they are

subject to unpredictable variation due to process variations, component aging, temperature and supply voltage variations.

In contrast digital delays comprise propagation delays through digital gates, and latencies where a digital process requires several clock pulses
5 before passing the signal. In the case of measuring time-of-flight the system clock is likely to be derived from a crystal, so the latencies are not expected to vary by more than a few parts-per-million.

It is an object of the present invention to mitigate the effects of analogue
10 and digital delays in time-of-flight ranging systems.

According to a first aspect of the present invention there is provided a method of operating a time-of-flight measurement system comprising a first part and a second part, both said parts having circuitry in the propagation path of signals transmitted by, and received by, the parts, the circuitry introducing
15 time delays in the propagation path, at least one of said first and second parts including means for determining the time-of-flight of the signals between the first and second parts, the method comprising calibrating the system by positioning the first and second parts within a known distance of each other, measuring the time-of-flight when the first and second parts are so positioned,
20 determining an error in the measured time-of-flight due to the propagation time delays in the circuitry by deriving the difference between the measured time-of-flight and a theoretical time-of-flight over the known distance and using the error for adjusting a subsequent time-of-flight measurement.

The first aspect of the present invention provides a method of operating:
25 a keyless entry system in which the first part is fixed and the second part is portable; a tracking system in which the first part is adapted to function as a range determining part and the second part is adapted to be carried by an object to be tracked; a vehicle security system comprising lockable security means responsive to locally generated signals and in which the first part is
30 adapted to be mounted in a vehicle and the second part is adapted to be carried by a vehicle user.

According to a second aspect of the present invention there is provided a system for performing a time-of-flight measurement, comprising a first part and a second part, both said parts having signal transmitting and receiving means for effecting communication with each other, the signal transmitting and receiving means introducing time delays in respective signal propagation paths, and at least one of the first and second parts including means for determining the time-of-flight of the signals between the parts, further comprising means responsive to the first and second parts being within a known distance of each other for calibrating the system, said means including means for measuring the time-of-flight over the known distance, means for determining an error in the measured time-of-flight by deriving the difference between the measured time-of-flight and a theoretical time-of-flight over the known distance and means for using the error for adjusting a subsequent time-of-flight measurement.

The second aspect of the present invention provides: keyless entry system in which the first part is fixed and the second part is portable; a tracking system in which the first part is adapted to function as a range determining part and the second part is adapted to be carried by an object to be tracked; a vehicle security system comprising lockable security means responsive to locally generated signals and in which the first part is adapted to be mounted in a vehicle and the second part is adapted to be carried by a vehicle user.

Calibrating/recalibrating the circuits every time, or at less frequent intervals, when a vehicle engine is turned on or off, a vehicle's driver door is opened or closed, or the second part is inserted in or removed from a receptacle inside a vehicle, enables a more accurate time of flight to be determined than would be the case if the vehicle and portable parts were calibrated once during their manufacture.

Additionally the method of calibration does not require the provision of specialist measuring equipment which means that it can be carried-out in a cost effective manner.

The present invention will now be described, by way of example, with reference to the accompanying drawings, wherein:

Figure 1 is a block schematic diagram of a passive keyless entry system;

5 Figure 2 illustrates diagrammatically how a relay attack can be effected;

Figure 3 is a block schematic diagram of a passive keyless entry system made in accordance with the present invention;

Figure 4 is a diagrammatic view of one embodiment of the present invention; and

10 Figure 5 is a diagrammatic view of a second embodiment of the present invention.

In the drawings the same reference numerals have been used to indicate corresponding features.

15 Referring to Figure 3 the illustrated passive keyless entry system is similar to that shown in and described with reference to Figure 1 and in the interests of brevity those parts already described will not be described again.

In Figure 3 a data base 60 is coupled to the microcontroller 18 in order to stored various characteristics of the system and components used in the system and which contribute to delaying the propagation of signals through the vehicle mounted first part and the portable second part.

In Figure 3 the challenge signal is shown as being transmitted by the transmitter 14 at time $T1$ and being received by the front end stage 26 at time $T2$. An UHF signal is transmitted by the transmitter 32 at a time $T3$ and is received by the receiver at a time $T4$. Assuming that the clocks of the parts 10 and 12 are synchronised and that there are no internal time delays so that $T2$ and $T3$ are the same, the time of flight (TOF) equals

$$TOF = \frac{T4 - T1}{2} \quad (1)$$

However because of the existence of internal analogue and digital delays which mean that $T2$ and $T3$ are different, equation (1) becomes:

$$TOF = \frac{(T2 - T1) + (T4 - T3)}{2} \quad (2)$$

For this equation it is assumed that the various times are correct and the signals are transmitted instantaneously, but in practice this is not the case. Consequently it is unreliable to assume that there is a fixed, unvarying time difference between $T2$ and $T3$. Since RF signals travel at approximately 300mm/nanosecond, delays in both the transmitter and receiver in TOF systems contribute a significant amount of both fixed and varying error in the measurement of TOF which can adversely affect the resolution if range measurement to within one or two metres is desired. Fixed delays occur due to the finite time for signals to move around the respective circuits and variable delays can be caused due to for example temperature effects (the automotive temperature range being -40°C to $+85^{\circ}\text{C}$), component aging, mechanical stress and supply voltage variations. Such delays, in the worse case may add the equivalent of hundreds of metres of error into the TOF calculation. Additionally, in manufacture, compensation for such delays can be made but such calibration corrections are based on certain criteria which may not apply in reality. Consequently for truly accurate measurements of TOF , calibration and recalibration needs to occur frequently and regularly throughout the lifetime of the vehicle mounted first part 10 and the portable second part 12.

The method in accordance with the present invention teaches that a calibration operation be carried-out frequently, for example on each use of the vehicle, once a day, once a week or once a month.

One method of carrying-out the calibration would be to place the portable part 12 in a fixed known location relative to the vehicle mounted part, the distance between the two parts being known. The error can be determined by comparing the measured range, that is the speed of light x time, and known range, thus: measured range - known range = error contribution.

The equivalent timing error is the error in range divided by the speed of light. In either case the error is stored in the data base 60 for use by the microcontroller when calculating TOF or range and operating or inhibiting the operation of a lock or other security device.

The need for calibration/recalibration is illustrated by a laboratory simulation of a passive keyless entry system in which a measured, unwanted, delay in each direction was equivalent to 510 metres whilst the theoretical delay was equivalent to 625 metres.

5 An advantage of determining the error contribution and making use of this contribution in calibrating the system is that no specialist measuring equipment is required. Also it avoids the complexity of determining the fixed and variable delays individually. However it is necessary to assume that the contribution of the variable delays is stable over the short term. The simple
10 and inexpensive calibration process facilitates frequent re-calibration, for example each time the portable part 12 is used, and thereby maintains confidence in the accuracy of the system.

Figure 4 illustrates the dashboard 62 of a vehicle. A holster, slot or other simple-to-use device 64 is provided in the dashboard 62 for holding the
15 portable part 12. Any other convenient location could alternatively be used. The vehicle mounted part 10 is located in close proximity, say less than one metre, of the device 64.

In operation the adjusted measured time-of-flight is compared with a threshold value and, if the result of the comparison is deemed to be
20 acceptable, an actuating signal for an external device is produced on the output 20 by the microcontroller 18, and if it is deemed to be unacceptable, production of an actuating signal is inhibited.

The device 64 may include an electrical connector or connectors coupled to the vehicle mounted part 10 and the vehicle electrical power supply
25 so that when the portable part 12 is inserted the clocks in the two parts 10, 12 can be synchronised and the battery 36, if rechargeable, can be recharged. Synchronising the clocks in the two parts 10, 12 will enable the clock edges to occur at exactly the same moment in time thus avoiding having to consider clock offset as a source of delay in the calibration process.

30 Figure 5 illustrates an embodiment in which the calibration is carried out within a vehicle without the need to provide a holster, slot or other retaining device. Once the portable part 12, which may be in a pocket or handbag (not

shown), is inside the vehicle it is assumed to be within one metre of the vehicle mounted part 10 and a calibration operation is initiated.

Errors will be time varying and hence it is appropriate to do the calibration often. In particular it is beneficial to perform the calibration when the user is about to leave the vehicle as this will minimise the time between calibration and the user returning to the vehicle and also the drift. The calibration process could be initiated in response to the engine being turned-off, driver door opening, removal of the portable part from a holster, slot or some similar type of device.

10 The calibration operation may be repeated several times in quick succession so that a mean value of measured range can be obtained.

In a situation of say a pool car where several people have access to the same vehicle and each person has their own second, portable part 12, the system has to be able to store in the data base 60 calibration values for each combination of the fixed first part and a respective one of the portable second parts 12. In order to be able to implement such a system each second part is given a unique address code which is included, for example as a header, in the UHF transmissions.

In order to provide a degree of calibration in a situation when a vehicle is used infrequently thereby reducing a risk to the vehicle being stolen, various algorithms may be stored in the data base 60 to introduce a progressive change in certain critical parameters affecting the variable delay incurred in the vehicle mounted part. As an example if the clocks in both parts are crystal controlled then an algorithm for compensating for frequency drift at various temperatures may be stored in the data base 60 and used as appropriate for correcting the clock frequency in the digital circuitry.

The method and system in accordance with the present invention may be used in combination with a wireless activation system disclosed and claimed in International Patent Application IB 03/05289 filed 19 November 2003, Applicant's reference PHGB020213WO. The wireless activation system disclosed uses repeated code sequences for communication between a transmitter device and a receiver device. By varying the sequence duration in

a synchronism at the transmitter device and receiver device, either by varying the number of symbols or chips in the sequence, or by varying the symbol or chip rate, it is made more difficult for an unauthorised party to detect the code sequences and relay the code sequences to achieve unauthorised activation
5 at the receive device.

Other applications to which time-of-flight measurements may be used are tracking systems such as toddler alarms for use in ensuring that toddlers do not stray too far when out roaming, for example when shopping, and systems for tracking doctors, patients and equipment on large sites such as
10 hospitals. In a parent/toddler or similar application the first part 10 would be carried by the parent and the second part 12 would be attached to the toddler. Calibration/recalibration could be effected by for example juxtaposing the first and second parts adjacent each other or spaced apart by a known distance or by introducing a known delay corresponding to a certain distance in the signal
15 propagation path.

In the present specification and claims the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. Further, the word "comprising" does not exclude the presence of other elements or steps than those listed.

20 From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the design, manufacture and use of time-of-flight ranging systems and component parts therefor and which may be used instead of or in addition to features already described herein.